(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number
WO 01/25925 A1

(51) International Patent Classification[7]: G06F 11/30, 12/00, 12/14, 13/00, 13/28, H04L 9/00, 9/32

(21) International Application Number: PCT/US00/26839

(22) International Filing Date:
29 September 2000 (29.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/157,472 1 October 1999 (01.10.1999) US
60/206,947 25 May 2000 (25.05.2000) US

(71) Applicant *(for all designated States except US)*: **INFRAWORKS CORPORATION** [US/US]; Suite 1100, 504 Lavaca Street, Austin, TX 78701 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FRIEDMAN, George** [US/US]; 7109 Montana Norte, Austin, TX 78731 (US). **STAREK, Robert, Phillip** [US/US]; 3609 Del Robles, Austin, TX 78727 (US). **MURDOCK, Carlos** [US/US]; 4517 Avenue F, Austin, TX 78751 (US).

(74) Agents: **CHRISTENBURY, T., Daniel et al.**; Schnader Harrison Segal & Lewis LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103-7286 (US).

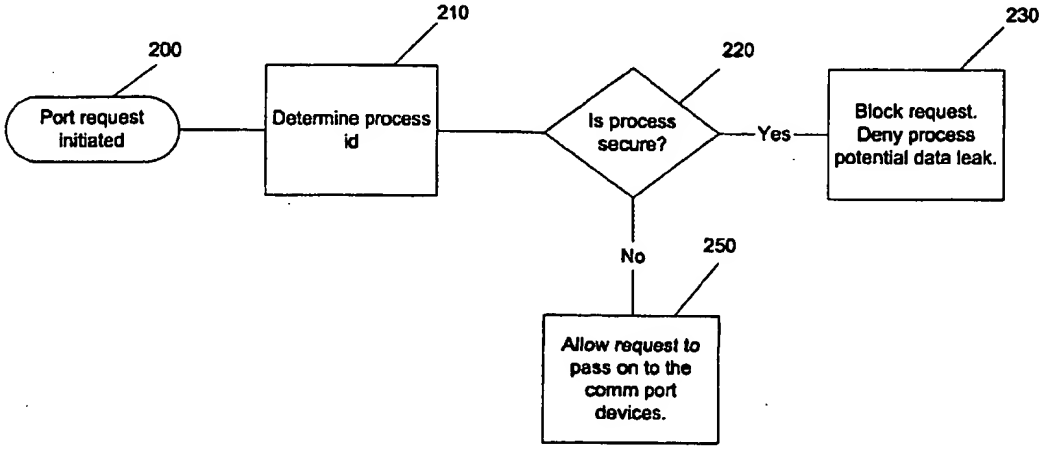
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PORT BLOCKING METHOD AND SYSTEM



(57) Abstract: A port blocking method (220) particularly applicable to a system in which protected data is segregated from other data, which allows for ports to be opened only by processes which do not have access to secured data (250) in order to ensure that applications using secured data do not imperil the security of secure data. In a preferred embodiment, port blocking method (220) is implemented in an application resident on the kernel level which monitors port requests and allows limited access to the port based on whether requesting processes are secure (220).

WO 01/25925 A1

PORT BLOCKING METHOD AND SYSTEM

Field of the Invention:

The invention relates to the protection of data stored in a computer, and more particularly, to data which has been secured and opened by non-secure applications where a high level application or operating system component acts to disable certain system resources in order to protect the security of data.

Background of the Invention:

In computer systems, processes may access many system resources, such as serial ports or connections to the Internet. In a situation in which secured data is being accessed by a non-secured application, a means must be developed by which the non-secured application can be restricted from performing operations which might compromise the security of the data.

It is known to open secure data in a system which is completely isolated from outside communications, which has no connection to means by which an unsecured application may, by accident or sabotage, compromise the secured data. It is also known to open secure data with secure applications, which are known to be free from the risk of accident or sabotage that would compromise the secured data. These solutions prevent the use of popular software applications to open secured data, or the use of a computer which is not disconnected from outside communications, and thereby are limited in their usefulness.

Summary of the Invention:

The invention discloses a port blocking method particularly applicable to a system in which secured data is transmitted to a recipient computer for use with non-secured applications. An illustrative embodiment of the invention comprises performing a security check on a process and blocking calls for use of a port if they come from a process using secured data. The tracking of secured processes may include determining whether and how often a secured process should be allowed to use a port. The security check may include determining whether the process is secured by consulting a secured process list and determining whether the resource should be available to the process requesting use of the resource.

Further disclosed is a port blocking system, secured data transmission system using

port blocking, computer-readable medium programmed to block port use, and a computer configured to block port use.

Description of the Drawings:

The invention is best understood from the following detailed description when read with the accompanying figures.

Figure 1 is an schematic diagram of a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 2 is a flow chart of a port request in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 3(a) is a flow chart of a port open request in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 3(b) is a flow chart of a port close request in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 3(c) is a flow chart of a security check in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Detailed Description of the Invention:

The invention disclosed prohibits certain processes from utilizing the port resources of the computer on which they are running. These may be secured processes for example, ones which have opened secure data. In a preferred embodiment of the invention, the status of a process as secured is determined by the processes presence on a list of secured processes.

In a preferred embodiment, as shown in Fig. 1, in a computer 100, a control application 110 runs on the kernel (ring 0) level 120 and applications 130 run on higher levels 140. When applications request access to port 150, control application 110 monitors and handles these access requests.

As shown in Fig. 2, in some computer systems, for example, Microsoft Windows NT and Windows 2000 operating systems, the port monitoring is able to intercept all port-related calls. When a port request is initiated 200, control application (110 in Fig. 1) intercepts that request, and determines the process id 210. The control application (110 in Fig. 1) in a preferred embodiment accesses a list of processes that are not allowed to open a port. The

process id is used to determine whether the process is secure (not allowed to open a port) 220. If it is secure, the request is blocked at 230. If it is not secure, then the request is passed on to the port 250.

As shown in Fig. 3(a), in some computer systems, for example, Microsoft Windows 95 and 98 operating systems, the port monitoring is able to intercept only open and close calls. In order to ensure that a process which has access to a port does not then become a secure process, a check must be performed on any process which is to become secure. When an open port request is initiated 300, control application (110 in Fig. 1) intercepts that request, and determines the process id 310. The control application (110 in Fig. 1) in a preferred embodiment accesses a list of processes that are not allowed to open a port. The process id is used to determine whether the process is secure (not allowed to open a port) 320. If it is secure, the request is blocked, 330, and the call is tracked 340. If it is not secure, then the request is passed on to the port and the process ID and port handle are tracked 350.

As shown in Fig. 3(b), when a close port request is initiated 360, control application (110 in Fig. 1) intercepts that request, and completes the call 362. Then the process ID and port handle is removed from the database of tracked open ports 364.

In addition to these operations on open port and close port requests, as shown in Fig. 3(c), when a process undergoes the security check which determines whether it will be secured, 370, its process id is checked against the database of tracked open ports 372. If the process has open ports, the process may not be made secure and the security check fails 374, and the security check is completed 376. If the process does not have open ports it will pass the security check and the process id will be added to the list of secured processes 378.

A further illustrative embodiment of the invention is directed to a port blocking system wherein certain processes are restricted from using a port, according to the methods provided herein. Further disclosed is a secured data transmission system having a port blocking component to prohibit certain processes from using a port according to the methods provided herein. Still further disclosed is a computer-readable medium programmed to block port use according to the methods provided herein. Still further disclosed is a computer configured to include a port blocking system to block certain processes from using a port according to the methods provided herein.

The terms "computer", "computer system", or "system" as used herein should be broadly construed to include any device capable of receiving, transmitting and/or using

information including, without limitation, a processor, microprocessor or similar device, a personal computer, such as a laptop, palm PC, desktop or workstation, a network server, a mainframe, an electronic wired or wireless device, such as for example, a telephone, an interactive television, such as for example, a television adapted to be connected to the Internet or an electronic device adapted for use with a television, a cellular telephone, a personal digital assistant, an electronic pager, and a digital watch. In an illustrative example, information is transmitted in the form of e-mail. Further, a computer, computer system, or system of the invention may operate in communication with other systems over a network, such as, for example, the Internet, an intranet, or an extranet, or may operate as a stand-alone system.

While the invention has been described by illustrative embodiments, additional advantages and modifications will occur to those skilled in the art. Therefore the invention in its broader aspects is not limited to specific details shown and described herein. Modifications may be made without departing from the spirit and scope of the invention. Accordingly, it is intended that the invention not be limited to the specific illustrative embodiments but be interpreted within the full spirit and scope of the appended claims and their equivalents.

[I / We] claim:

1. A port blocking method for securing data comprising:

a port request detection step of detecting a port request for use of a port sent by a process;

a process identification step of determining the identity of said requesting process;

a process check step of determining if said process should be permitted to access said port; and

a permit/deny step of allowing said port request to be fulfilled if said process should be permitted to access said port and denying said port request if said process should not be permitted to access said port.

2. The method of claim 1 where said process check step comprises:

a secure process list check step of determining whether said process appears on a list of secure processes.

3. A port blocking method for securing data comprising:

a port request detection step of detecting a port request for use of a port sent by a process;

an open port process identification step of, if said port request is an open port request, determining the identity of said requesting process;

an open port process check step of, if said port request is an open port request, determining if said process should be permitted to open said port;

an open port permit/deny step of, if said port request is an open port request, allowing said open port request to be fulfilled and tracking said open port request if said process should be permitted to open said port and denying said port request if said process should not be permitted to open said port;

a close port process completion step of, if said port request is a close port request, completing said port request; and

a close port logging step of, if said port request is a close port request, logging the closing of said port.

4. The method of claim 3 where said open port process check step comprises:

a secure process list check step of determining whether said process appears on a list of secure processes.

5. The method of claim 3 where said tracking of said open port request comprises keeping a log of process ID and returned port handle for said open port request, and said close port logging step of tracking the closing of said port comprises removing from said log said record of process ID and returned port handle for that port close request.

6. The method of claim 5 further comprising:

a security check step comprising the steps of checking whether a process has open ports, and denying security clearance for a process with open ports, and allowing security clearance for a process with no open ports.

7. The method of claim 6 where said open port process check step of comprises determining if said process identity appears on a secured process list, and where said step of allowing security clearance for a process with no open ports comprises the step of placing said process on said secured process list.

8. A port blocking system wherein said port blocking system operates to detect a port request for use of a port sent by a process; determine the identity of said requesting process; determine if said process should be permitted to access said port; and allow said port request to be fulfilled if said process should be permitted to access said port and deny said port request if said process should not be permitted to access said port.

9. A port blocking system wherein said port blocking system operates to detect a port request for use of a port sent by a process; if said port request is an open port request, determine the identity of said requesting process; if said port request is an open port request, determine if said process should be permitted to open said port; if said port request is an open port request, allow said open port request to be fulfilled, track said open port request if said process should be permitted to open said port, and deny said port request if said process should not be permitted to open said port; if said port request is a close port request, complete said port

request; and if said port request is a close port request, log the closing of said port.

10. A secured data transmission system having a port blocking system which operates to detect a port request for use of a port sent by a process; determine the identity of said requesting process; determine if said process should be permitted to access said port; and allow said port request to be fulfilled if said process should be permitted to access said port and deny said port request if said process should not be permitted to access said port.

11. A secured data transmission system having a port blocking system which operates to detect a port request for use of a port sent by a process; if said port request is an open port request, determine the identity of said requesting process; if said port request is an open port request, determine if said process should be permitted to open said port; if said port request is an open port request, allow said open port request to be fulfilled, track said open port request if said process should be permitted to open said port, and deny said port request if said process should not be permitted to open said port; if said port request is a close port request, complete said port request; and if said port request is a close port request, log the closing of said port.

12. A computer comprising a communications port and configured to protect secure data by including a port blocking system which operates to detect a port request for use of a port sent by a process; determine the identity of said requesting process; determine if said process should be permitted to access said port; and allow said port request to be fulfilled if said process should be permitted to access said port and deny said port request if said process should not be permitted to access said port.

13. A computer comprising a communications port and configured to protect secure data by including a port blocking system which operates to detect a port request for use of a port sent by a process; if said port request is an open port request, determine the identity of said requesting process; if said port request is an open port request, determine if said process should be permitted to open said port; if said port request is an open port request, allow said open port request to be fulfilled, track said open port request if said process should be permitted to open said port, and deny said port request if said process should not be permitted to open said port; if said port request is a close port request, complete said port request; and if

said port request is a close port request, log the closing of said port.

14. A computer-readable medium programmed to protect secure data by implementing a port blocking system which operates to detect a port request for use of a port sent by a process; determine the identity of said requesting process; determine if said process should be permitted to access said port; and allow said port request to be fulfilled if said process should be permitted to access said port and deny said port request if said process should not be permitted to access said port.

15. A computer-readable medium programmed to protect secure data by implementing a port blocking system which operates to operates to detect a port request for use of a port sent by a process; if said port request is an open port request, determine the identity of said requesting process; if said port request is an open port request, determine if said process should be permitted to open said port; if said port request is an open port request, allow said open port request to be fulfilled, track said open port request if said process should be permitted to open said port, and deny said port request if said process should not be permitted to open said port; if said port request is a close port request, complete said port request; and if said port request is a close port request, log the closing of said port.

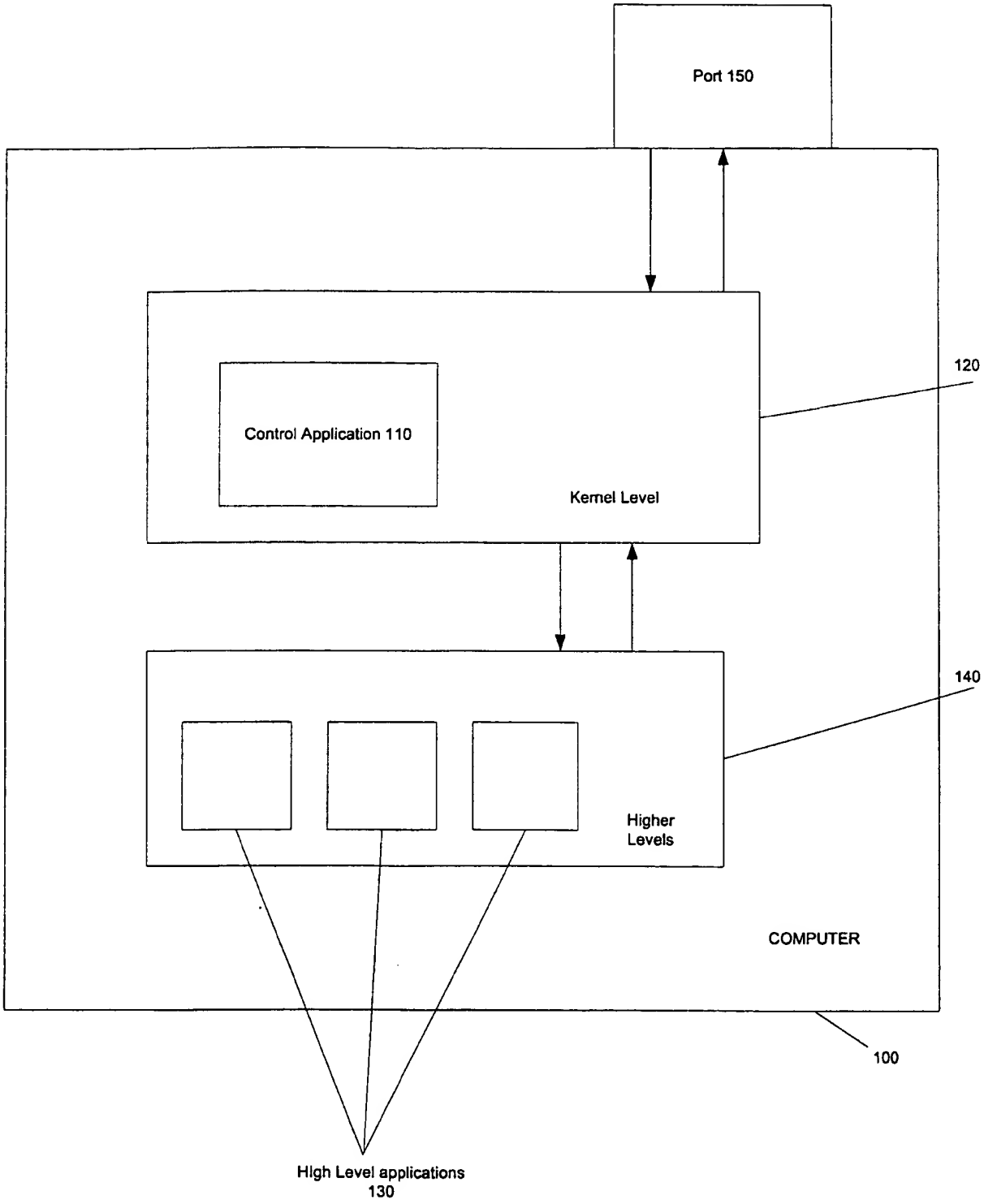

Port 150
Control Application 110
Kernel Level
120
140
Higher Levels
COMPUTER
100
High Level applications 130

FIG. 1

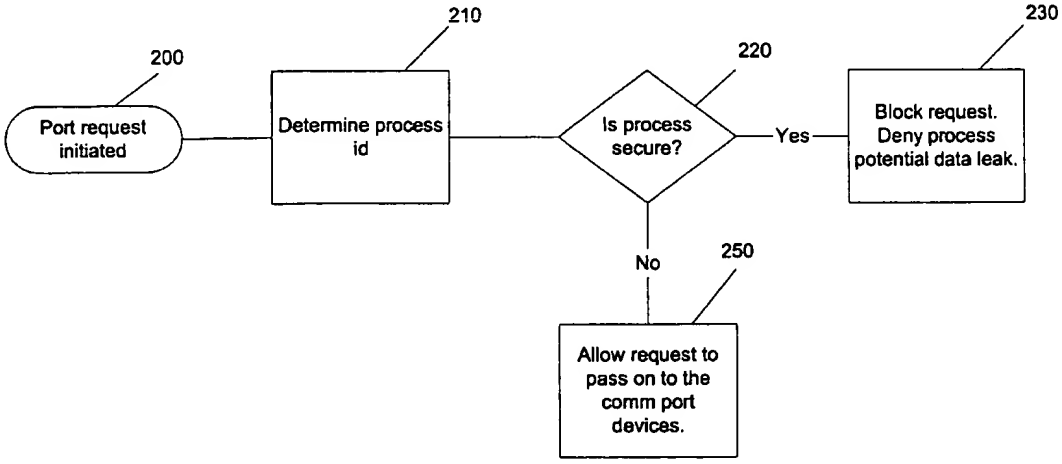

200
Port request initiated
210
Determine process id
220
Is process secure?
Yes
230
Block request. Deny process potential data leak.
No
250
Allow request to pass on to the comm port devices.

FIG. 2

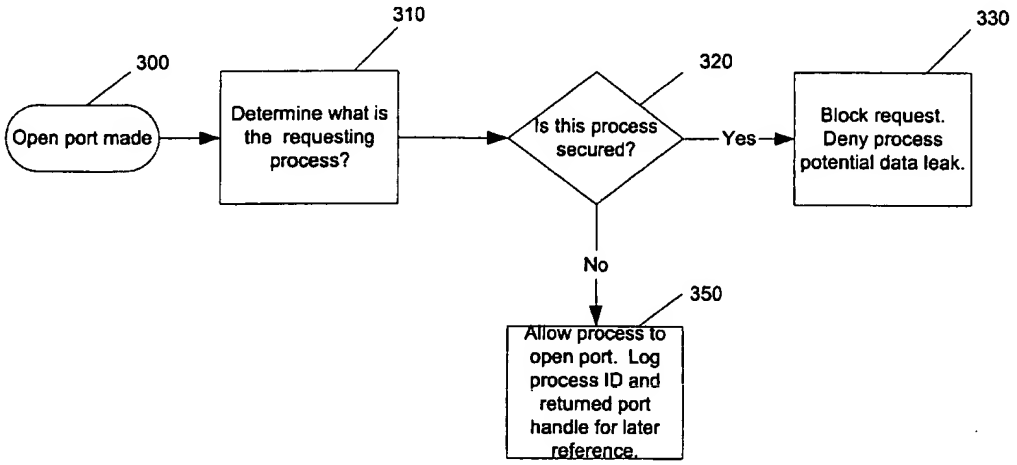


FIG. 3a

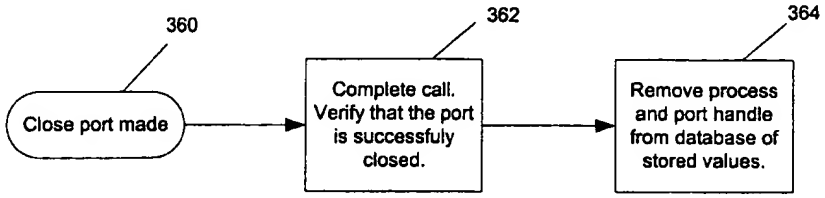


FIG. 3b

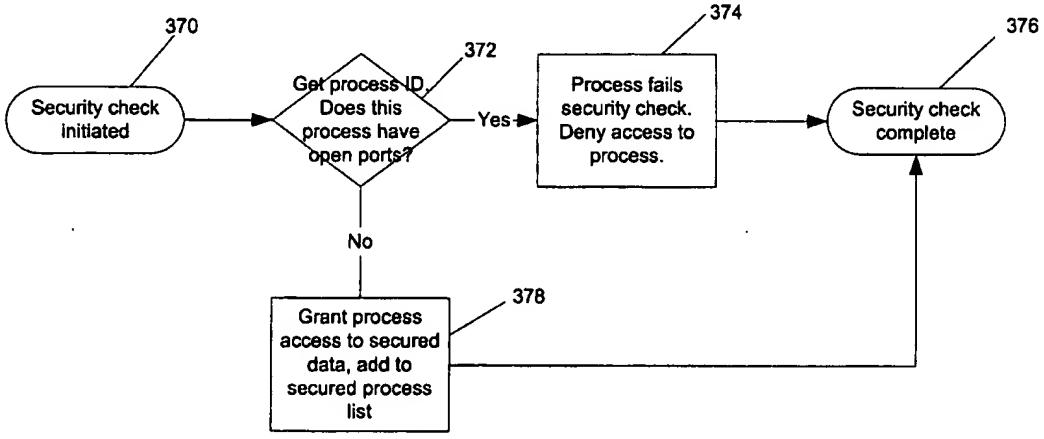


FIG. 3c

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/26839

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/30, 12/00, 12/14, 13/00, 13/28; H04L 9/00, 9/32
US CL : 713/200, 201; 345/518; 365/230.05; 711/149, 152, 163
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201; 345/518; 365/230.05; 711/149, 152, 163

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,845,068 A (WINIGER) 01 DECEMBER 1998, COL3, LINES 32-67, COL 4, LINES 5-10, 64-67, COL 5, LINES 1-22	1-15
---		---
Y		1-15
Y	US 5,892,903 A (KLAUS) 06 APRIL 1999, SEE ENTIRE DOCUMENT	1-15
Y	US 5,615,340 A (DAI ET AL) 25 MARCH 1997 SEE ENTIRE DOCUMENT	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 02 DECEMBER 2000	Date of mailing of the international search report 22 DEC 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GAIL HAYES Telephone No. (703) 305-9618

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/26839

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

BRS TEXT (USPAT, DERWENT, JPO, EPO, IBM TDB's), DIALOG (FILE COMPSCI), CORPORATE RESOURCE NET

search terms: port, ports, block, allow, deny, denied, permit, permitting, allowing, secure, private, confidential, protected, security, classified